Departmental GISRA Report Review

I've gathered together my comments regarding the Department's GISRA report. I concentrated primarily on the information in the executive summary, although I did use the main report to determine the source of some of the information reported. Therefore, all comments refer to the executive summary unless noted otherwise.

Overall, the summary provides the highly optimistic counter to the OIG's GISRA report. Discrepancies and issues were mentioned, but nowhere nearly in the same depth as accomplishments and planned goals. To their credit, the main report does go further in depth into outstanding issues and concerns, but the executive summary as definitely biased towards the congratulatory.

Some specific items:

- Sect 1.3 - Current IT Security Efforts (p.4) - To the uninitiated, it would certainly seem that the Department has accomplished more than it actually has. The IT Security Policy is, "in the final stages of approval," even though it went through a major rewrite which none of the POs have had the chance to review yet. The discuss how, "Tactical plans detail the next steps for program subelements, including IT security compliance, CIP, IT security metrics, [etc.]," and that Various guidance documents address execution of C&A activities such as security controls, contingency planning, security testing and evaluation, [etc.]." They follow this, however, by stating that these "documents have been disseminated throughout the Department." In reality, very few of these documents have been released, whereas many of them are still in draft format undergoing Departmental review. Although I understand the desire to take credit for the massive effort in documenting all of ED's processes and procedures, they should still call it like it is, that most of these documents are in draft status, and will be released to the Department pending review and approval.
- Sect A.1 - Security funding (p.5) - To my understanding, the $565,000 spent by FSA on risk assessments only includes the BAH assessments. Several other risk assessments were completed by separate contractors both before and simultaneously with the BAH assessments.
- Sect A.2 - System and Program Inventory (p.6) - ED should also mention that an accomplishment of their Department-wide inventory and inventory guidance was the baseline definition of what ED would use to determine a high/medium/low rating for a system's sensitivity categories (confidentiality, integrity, and availability). This definition formed the core of determining the security requirements of a system (Major Application vs. application), allowed the creation of the Department's tiering system, and eased the comparison of risk assessment findings. This was mentioned in the main report, but was not given its due credit.
- Sect A.3 - Material Weakness (p.7) / Sect B.2 - Security Life Cycle (p.9) - Nowhere, neither in the executive summary nor in the main report, was any mention made of FSA's SLC. The GISRA report goes through great pains to discuss how the Department is working on creating an SDLC that contains C&A requirements throughout the lifecycle, culminating in the certifying and accrediting the system before the system begins operation. FSA already has this strategy implemented in their SLC, and in fact, is using the methodology in their SLC for everything up to certifying and accrediting the systems, the latter not taking place only because it must rely on the Department to determine how it wants to perform C&A. FSA should get credit for leading the way in this area, and I'm fairly certain it is the only reason

why there are any systems that take credit for life cycle accomplishments in the self-assessment graph in the main report.

- Table A-20 - POA&M Results (Main report, p.35) - This table needs to be reviewed. Should it include quarterly information in an annual report? Also, the last two rows need to be re-entered; the contents do not seem to match the descriptions for the cells.
- Table B-1 - Security Life Cycle (p.10)/Table C-9 - FSA Security Figures (p.16)- As a comparative to the Departmental information, here is how FSA contributed to the Department's numbers:

	FY02 # systems/92	FY02 %	FSA systems	% of compliant systems
RA	92/92	100%	17	18.5%
Assigned risk level	92/92	100%	17	18.5%
Updated SSP	36/92	44%	12	33%
C&A complete	0	0%	0	0%
Operating w/o C&A	92/92	100%	17	18.5%
Integrated SLC	0	0%	0*	0%*
Tested sec controls	49/92	60%	10	20.4%
Contingency Plan	40/92	49%	11	27.5%
Tested Cont. Plan	37/92	45%	10	27%

*Based on lack of Departmental SLC

As you can see, in every category, FSA has a higher share of systems in compliance, underlining our stance as the Department's security leaders.

- Sect C.2 - Supporting Services Security (p.19) - Although they provide the number of contractor facilities/operations, and the number of these that were reviewed for security in their contracts, nowhere does it discuss the results of that review. A third row needs to be added to the results table showing the number of reviewed contracts with security wording integrated in the contracts.
- Lastly (a minor point) - the Table of Contents for the main report needs to be updated.